UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Financial Institutions Cases	MDL No. 14-2522 (PAM/JJK) **MEMORANDUM OF LAW IN SUPPORT OF FINANCIAL INSTITUTION PLAINTIFFS' MOTION FOR CLASS CERTIFICATION AND FOR APPOINTMENT OF CLASS REPRESENTATIVES AND CLASS COUNSEL [REDACTED VERSION]**

TABLE OF CONTENTS

Page

I. PRELIMINARY STATEMENT

Financial Institution Plaintiffs 6+7*"4.&488(19 move for: (1) certification under Federal Rule of Civil Procedure 23(a) and 23(b)(3) of a class of all entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by Target on December 19, 2013 6+)*"((19; (2) appointment of Plaintiffs Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain as Class Representatives; and (3) appointment under Rule 23(g) of Zimmerman Reed PLLP and Chestnut Cambronne PA as Co-Lead Class Counsel and each of the firms identified in the)5-#&'(May 22, 2014, and June 2, 2015, Orders (ECF Nos. 74 & 436),[1] as Lead and Liaison Counsel and members of the Executive and Steering Committees for the Financial Institution track, as Co-Class Counsel.[2] Additionally, as part of any order certifying the Class, Plaintiffs request that the Court expressly reserve the right of Class members, on the basis of any liability determination, to seek additional compensable damages beyond the class-wide damages being sought.

As Defendant Target Corp. 6+!"#$%&1 or the +)50:".19 has implicitly conceded by its recent attempt to effectuate a class-type settlement and release with the putative

[1] References to +;), <5=>>1 are to filings in MDL No. 14-2522 (PAM/JJK). References to the +)50:*"4.&1 or +)50:*=1 are to ECF No. 163. Also, unless otherwise indicated, internal quotations and citations have been omitted from, and emphases added to, cited sources.

[2] Counsel for Defendant has stated that it will not oppose the proposed appointment of counsel as proposed here.

Class via MasterCard, this case is appropriate for certification as a class. Moreover, Plaintiffs have met their burden under a +#4$5#5-("."*/(4(1 to establish the requisite elements under Rules 23(a) and (b)(3). 7*"4.&488(' motion is well supported by the evidence developed through (ongoing) discovery and the expert reports of Neil Librock, a former Executive Vice President and Senior Credit Officer at Wells Fargo Bank N.A. (the +?42#5@A Declaration19 and Robin Cantor, Ph.D. (the +)".&5# B%:5#&19C which are contemporaneously filed. Mr. Librock and Dr. Cantor have opined on the common impact of the Breach (defined below) across all Class members (Librock Declaration/Cantor Report) and the ability to calculate class-wide damages based on discovery evidence (Cantor Report).

The Class is Ascertainable. The class definition comprises objective, definite criteria sufficient for the Court to determine whether a given entity is a Class member. In fact, all putative Class members can be identified at the outset from !"#$%&'(data, and reports and notifications about the Breach.

Numerosity is met. The Class is sufficiently numerous, containing thousands of institutions. Joinder of all parties would be impracticable.

Typicality and Adequacy are Established. 7*"4.&488(' claims are typical of the)*"((('(C as both accrue based on the same underlying conduct by Target and seek the same relief. 7*"4.&488(' interests are therefore directly aligned with those of the Class. Moreover, as is evident from the prosecution of this litigation to date, Plaintiffs and their proposed lead and class counsel have demonstrated their adequacy to serve the Class.

Common Questions of Law and Fact Predominate. The)*"((' claims raise numerous common issues of fact and law. All claims will commonly rise or fall on the basis of what can be proven about !"#$%&'(retention of data and its conduct in permitting the Breach, and whether this conduct violated Minnesota statutory and common law. Common evidence D that the Breach resulted from !"#$%&'(failure to employ proper security protocols and personnel, !"#$%&'(failure to heed clear and specific warnings of an imminent security threat, and !"#$%&'(inexplicable decision to disable security features that could have stopped or minimized the Breach D will drive the resolution of ***every*** Class 0%02%#'(claim. There is no ambiguity in !"#$%&'(obligation to safeguard the)*"((' financial data under Minnesota statutory and common law. Indeed, with respect to card data security, Target owed each Class member the same duty of care, and !"#$%&'(security failings either did or did not breach that duty to every Class member. Likewise, if Plaintiffs establish that Target violated the Plastic Card Security Act (the +7)EF19C Minn. Stat. § 325E.64, that liability finding would apply class-wide. Any differences at issue in this litigation will concern amounts or types of damages D but such differences do not preclude certification.

Matters of damages and causation will also turn on fundamentally common evidence. As described in the Librock Declaration, the Breach commonly impacted all entities that issued compromised payment cards. These institutions D the Class members D were required to respond pursuant to regulatory obligations and to mitigate their financial exposure from the breach. Responses included, among other things, cancelling and reissuing cards, reimbursing customers for fraudulent transactions, and undertaking

additional customer service. Each of these responses is ***specifically recognized*** as reasonable under the PCSA. *See* Minn. Stat. § 325E.64, subd. 3. Damages for reissuance costs and fraud losses can be calculated in a formulaic manner from common evidence on a class-wide basis, as described in the Cantor Report. These categories of damages are consistent with 7*"4.&488(' theories of liability under both the PCSA, which specifically provides compensation for reissuance and fraud losses, and negligence.

A Class Action is Superior. A single adjudication of !"#$%&'(alleged unlawful conduct entailing all Class 0%02%#(' claims is vastly superior to the prospect of thousands of financial institutions being required to try, upon remand, the same questions against the same defendant in potentially separate proceedings before dozens of courts across the United States.

Therefore, respectfully, the Court should certify this Class.

II. STATEMENT OF FACTS

A. Common Facts Establish Target's Liability

Discovery to date has confirmed that the breach of !"#$%&'(centralized computer system in November and December of 2013 (the +!"#$%& G#%"@H1 or the +G#%"@H19 was the direct and foreseeable consequence of !"#$%&'(longstanding lackadaisical practices and corporate attitudes toward securing sensitive payment card data. Discovery (which is still ongoing and continues to reveal details related to !"#$%&'(cybersecurity failings) has established that Target hired ill-equipped employees to oversee its data security systems, maintained woefully deficient security programs, repeatedly ignored pre-Breach warnings about malware intrusions and took steps to limit %0:*5/%%(' ability to secure

data in busy periods to avoid disrupting its flow of profits. Common evidence, applicable class-wide, will show that, due to its egregious and repeated card data security failures, !"#$%&'(own conduct led to the Breach and caused massive losses to financial institutions.

B. Target Ignores Warnings about Malware Attacks on POS Terminals Months Before the Breach

The evidence already available to date, reveals that both before and during the Breach, Target maintained substandard cybersecurity practices, which allowed the inception and caused it to spiral from a controllable event with minimal losses into one of the largest data security breaches in United States history.

!"#$%&'(cybersecurity deficiencies were obvious well before the Breach. In particular, Nickolas Kemske, testified that former Target Information Protection and Cyber Security Manager,[3] although a number of teams at Target were responsible for responding to a security breach, these teams had fundamental difficulties communicating and collaborating.[4] According to Kemske, there was no formal process or procedure in place for following up on potential cybersecurity threats or for communicating threats to !"#$%&'(senior executives.[5]

---

[3] Kemske Dep. at 62:1-63:7, submitted as Exhibit A to the Declaration of J. Gordon Rudd, Jr., In Support of the Financial Institution 7*"4.&488(' Motion For Class Certification, Appointment of Class Representatives and Appointment of Co-Lead and Co-Class Counsel 6+B-II J%@*=19= +;K=>>1 refers to an exhibit to the Rudd Decl.

[4] Ex. A at 111:3-13; 112:15-117:16.

[5] *Id*. at 253:6-254:14; 278:11-24.

Another witness, Michael Salters, Group Manager for !"#$%&'(Security Operations Center, testified that in April 2012, Target discovered unencrypted payment card information dating back +"& least six or seven /%"#(1 on servers in 292 Target stores.[6] Despite finding this unencrypted card data, Target failed to take any action (it +I#5::%I the 2"**19 for nearly six months until the end of September 2012.[7] As a result of its five-month delay, Target postponed signing its 2012 PCI compliance attestation.[8] Even worse, Target continued to retain unencrypted payment card data on its system. Specifically, unencrypted card data ***dating back almost ten years*** was found in plain text on !"#$%&'(servers during the investigation of the Breach.[9]

Two third-parties conducted studies of !"#$%&'(cybersecurity environment in the first eight months of 2013. The first study, by Deloitte in April 2013, found clear

---

[6] Ex. B (Salters Dep.) at 30:21-33:22; 49:24-50:22; 86:13-87:23); Ex. C at 351. For citations to exhibits containing Bates-labeled documents, all page number references are to the Bates pagination rather than the original pagination.

[7] Ex. B at 80:20-81:17; 97:3-12; Ex. D (Brinkhaus Dep.) at 71:3-14; 175:24-179:5.

[8] *See* Ex. B at 122:3-25; Ex. C at 355 6+7#52*%0("((%((4.$L&H% incident put Target at risk ***of becoming PCI non-compliant*** L= Remediation efforts began just prior to the annual review date for PCI Attestation. If the incident was ***correctly assessed in May*** L !"#$%& would not have delayed signing [its PCI F&&%(&"&45.M=19= The Payment Card Industry Data Security Standards 6+7)N JEE19 are information security requirements promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed, or transmitted and require merchants like Target to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies. Compl. ¶19.

[9] Ex. E at 081.

deficiencies and made several recommendations. Of particular note, Deloitte found an +0"M2(%.@% of advanced malware detection tools and lack of focused roles and responsibilities to manage advanced threat identification, tracking, triaging and #%(:5.(%=1[10] The second study, by the Chertoff Group in August 2013, resulted in nineteen recommendations that, if implemented, would have prevented or minimized the impact of the Breach.[11] One recommendation, for example, was to use whitelisting D a process that specifically defines what programs are allowed to run and blocks all other programs (such as malware) automatically.[12] Subsequently, Target actually deprioritized whitelisting and failed to engage in serious discussions about its implementation, which Beth Jacob, !"#$%&'(CIO, acknowledged after the Breach as a +O4((=1[13]

In January, April, and August 2013, Target received specific warnings about malware targeting point-of-service 6+7PE19 terminals (i.e., in-store registers) D the same devices infected by malware in the Breach.[14] Target noted the threat and its applicability to the Company, circulating a +!H#%"& Assessment of POS G#%"@H%(1 amongst its cybersecurity teams.[15] However, Target took no action to protect its system from a POS

[10] Ex. F at 734.

[11] Ex. G at 032, 035-038.

[12] *Id*. at 038 & 090.

[13] Ex. H.

[14] Ex. I; *see also* Ex. J 6+F QR4**)H"4.' Analysis of the 2013 Target Data Breach).

[15] Ex. K.

intrustion.[16] In fact, months after being made aware of this threat, Target had not defined roles for responding to POS malware or conducted any internal security audits related to POS terminals and malware threats.[17] Also in 2013, Target specifically became aware of +G*"@A7PE1 malware D the same type of malware used in the Breach.[18] Five months before the Breach, !"#$%&'(Global Intelligence Department distributed a report entitled +G*"@A7PE Threat F((%((0%.&1 to !"#$%&'(cybersecurity teams that described, in detail, how BlackPOS works and provided variants of the file names and unique signatures to identify the malware.[19] Just like the warnings of POS malware, the specific BlackPOS information went unheeded. Rather, !"#$%&'(cybersecurity team noted that +&H4([BlackPOS] information is reviewed by the team, ***but no real action is being taken***=1[20] Thus, even months after it identified the threat of BlackPOS, continued to ignore this serious risk in its data security operations which could have catistrophic consequences D which is exavlty what occurred in the Breach.[21]

---

[16] Ex. A 228:19-229:23.

[17] *Id*. at 233:21-234:9.

[18] In an article posted by Brian Krebs to his cybersecurity blog, Krebs identified the malware used to attack Target as +.%"#*/ identical to a piece of code sold on cybercrime forums called ***BlackPOS***=1 Ex. L at 372 (emphasis in original). Jenny Ley, a Director of Risk Intelligence at Target, forwarded the blog post to a colleague and described Kr%2(' post as +%K&#%0%*/ detailed (and "@@-#"&%9=1 *Id*. at 370.

[19] Ex. M.

[20] Ex. N.

[21] Ex. A 275:21-278:10.

C. Target Inexplicably Disables Security Features

Not only did Target maintain a culture of indifference to safeguarding sensitive financial data from warned POS malware attacks but in the days leading up to the Breach, Target made three inexplicable decisions that allowed the Breach to occur and greatly increase its severity. First, in October 2013, Target disabled and removed key security features provided by Symantec, !"#$%&'(anti-virus provider, and kept them disabled and removed +-.&4* after black ,#4I"/=1[22] Second, Target installed a FireEye application, but incredibly only implemented ,4#%;/%'(malware +I%&%@&45. 05I%C1 and not its malware prevention features, which was designed to pr

event malware from entering !"#$%&'(system.[23] Third, Target failed to integrate FireEye properly into its alert-generating system, guaranteeing that ,4#%;/%'(actual detection of BlackPOS on !"#$%&'(systems on December 2, 2013, went unheeded.[24] Target also failed to implement newer available technology to detect certain types of malware.[25] Allowing any one of these systems to operate in their normal course would have limited or prevented the Breach. !"#$%&'(pre-Breach conduct is consistent with discovery establishing T"#$%&'(willingness to de-prioritize cybersecurity in favor of the chance for higher revenue. For example, Target implemented a +(/(&%O 8#%%S%1 (which

[22] Ex. O at 795.

[23] Ex. P (Salters II Dep.) at 53:4-17; 62:14-63:2; Ex. Q (Bobo Dep.) at 24:21-25:5; 65:18-66:5.

[24] Ex. P at 60:12-62:5; 177:22-178:20.

[25] Ex. P at 53:19-55:20.

makes it much more difficult to make changes to !"#$%&'(computer and security systems) during seasons where Target generated the most revenue.[26] Notably, according to the deposition testimony of Jeffrey Jaynes, an Engineering Consultant in Target Technology Services, Target implemented such a system freeze during the Breach D from approximately October 2013 to January 2014.[27] Target was very interested in accepting the)*"((' financial data to drive profits but had no interest in safeguarding it from known threats.

D. Target's Negligence Exposes the Class's Financial Data Causing the Class to Suffer Massive Losses

Against the backdrop of !"#$%&'(culture of indifference to safeguarding financial data and pre-Breach profit measuring decisions, the Breach itself began on or around November 12, 2013, when intruders used the credentials of !"#$%&'(refrigeration vendor, Fazio Mechanical Services, Inc. 6+,"S4519C to log onto !"#$%&'(servers.[28] Fazio was given access to !"#$%&'(system using construction management software, which could be accessed by ,"S45'(employees through Target-issued log-in credentials.[29] Target was ,"S45'(only customer that hosted its construction management software on !"#$%&'(own system (as opposed to the software being hosted on a third-party server), which provided

[26] *See* Ex. D at 36:2-39:14.

[27] Ex. R (Jaynes Dep.) at 35:24-36:7; 140:1-143:22.

[28] Ex. S at 423; Ex. T (Mitsch Dep.) at 10:13-18; 154:9-24.

[29] Ex. T at 76:2-79:20; 84:5-85:22; 94:8-97:11.

the intruders, through Fazio, direct access to !"#$%&'(system.[30] Notwithstanding the incredible access given to Fazio, Target never conducted a risk assessment of Fazio (from the start of Fazio and !"#$%&'(relationship in 2006 through the Breach), despite !"#$%&'(admission that such vendor assessments should be completed.[31] Further, Target did not, at any time prior to the Breach, require Fazio to employ a two-factor authentication system in order to log-in, notwithstanding !"#$%&'(purported policies and industry standards.[32] Requiring two-factor authentication would have significantly impeded, if not entirely thwarted, the intrusion.[33]

Gaining access to !"#$%&'(systems was not overly complicated. The intruders sent a +:H4(H4.$ %O"4*1 to a Fazio employee. Once the employee opened the email, the intruders had access to ,"S45'(computers which in turn enabled them to obtain that %O:*5/%%'(log-in credentials to !"#$%&'(system.[34] Incredibly, the log-in credentials of this lone vendor D who was not required to adhere to any advanced security protocol by Target D provided virtually limitless access to all of !"#$%&'(servers. After entering !"#$%&'(servers, the hackers gained access to the store networks and installed malware

---

[30] *Id*. at 157:4-9.

[31] Ex. U (Hanson, Dep.) at 159:19-163:1; 174:1-177:4; Ex. T at 33:7-8; Ex. E at 019 & -030.

[32] Ex. T at 121:9-18; Ex. U at 85:5-10 & 116:7-117:14; Ex. V at 293; *see also* Ex. E at 038 6+!"#$%& ***did not*** store or collect . . . access logs in a manner consistent with the PCI JEE1T+I%84@4%.@4%(related to both scope and retention of these logs were :#%(%.&19=

[33] Ex. U at 100:8-101:25.

[34] Ex. T at 177:10-179:14.

onto !"#$%&'(POS terminals that collected the)*"((*(sensitive payment card data from the termin"*(' memory from November 28 to December 15, 2013.[35] Intruders were able to scrape the POS memory because, according to John Deters, an Engineering Consultant in Target Technology Services, Target retained unencrypted card data, including full magnetic stripe data, on the POS terminals beyond the sales transaction.[36] The malware then stored the compromised payment card data on !"#$%&'(systems for several days, before transmitting the data to the 4.&#-I%#(' third-party servers.[37]

E. "Funny thing was that this one looked kinda suspicious to me"

Target ignored multiple alerts and warnings that could have terminated the Breach before the)*"((*(information was compromised. As early as November 24, 2013, Symantec detected malicious password-stealing software related to the Breach, specifically a +(%@-#4&/ #4(A1 classified as [redacted] on !"#$%&'(server.[38] Target, however, failed to take any action to stop the Breach. On November 25, 2013, Target received an alert for unauthorized activity on its POS terminals, which led a Target Security Operations Center employee to note in an email, ***+Funny thing was that this one looked kinda suspicious to me. Looks like someone s using a service account***

[35] Ex. S at 424-425.

[36] Ex. W (Deters Dep.) at 72:8-74:21; 76:1-76:5; 124:2-8; 182:13-186:19.

[37] Ex. S at 425-426.

[38] Ex. E at 020 & 023; Ex. X.

to access all the registers in one store[39] Despite clear recognition of an attempt to access POS registers and the payment card data thereon, Target continued to sit on its hands while the busy shopping season continued. The following day, on November 26, 2013, E/O".&%@'(antivirus software again detected password-stealing malware.[40] Instead of immediately acting, however, Target chose to +H5*I 5881 on necessary changes for concerns of disrupting Cyber Monday.[41] This delay extended until at least December 13, 2013, if the change was ever made.[42] Perhaps most damning, as early as November 30, 2013, and again on December 2, 2013, FireEye, the application purchased by Target to help detect malware, ***detected the presence of the malware*** used in the Breach.[43] Target, however, had failed to integrate FireEye into its security alert application, [redacted] which was the application that sent security alerts to Target. Because Target chose not to integrate FireEye and [redacted] these alerts were not being monitored, and the malware detection tool was rendered useless.[44] Despite the alarms, the Company sat

[39] Ex. Y.

[40] Ex. E at 023; Ex. X.

[41] Ex. Z.

[42] Ex. R at 162:23-164:16; Ex. AA.

[43] Ex. E at 020; Ex. BB.

[44] Ex. P at 60:12-62:5.

idly while the intruders collected the)*"((' information and only reacted after it was contacted by the U.S. Secret Service on December 12, 2013.[45]

In the end, approximately 40 million payment cards were compromised as a result of the Breach.[46] In addition, personal information, including addresses, phone numbers, and email addresses, of up to 70 million customers was also taken.[47]

F. An Independent Investigation Concludes That Target Is Responsible for the Breach

Verizon, the independent forensic investigator of the Breach, concluded that Target was responsible for the Breach, based on its multiple security failures including among other things: a lack of outbound internet restriction; lack of proper network segmentation; [redacted][48] Moreover, Verizon indicated that Target accepted too many risks and that Target Information Protection 6+!N719 lacked the skills to fulfill its job functions.[49] Verizon also concluded that Target was not in compliance with the PCI-DSS in several material respects when the Breach occurred. Verizon determined that the Breach would not have occurred without !"#$%&'(security

[45] Ex. E at 023-024.

[46] *See* Ex. W at 182:13-186:19; Ex. E at 028 (Verizon determined that 39,292,617 unique payment cards were deemed at risk).

[47] Ex. CC.

[48] Ex. E at 018-019.

[49] Ex. DD.

failings.[50] MasterCard relied upon the Verizon Report for determining !"#$%&'(liability under its account data compromise 6+FJ)19 program, which MasterCard and Target both used as a basis for their failed proposed Settlement Agreement.[51]

G. Every Class Member Was Forced to Respond Once Alerted of the Breach

Most Class members learned about their compromised cards through alerts sent by card brands MasterCard and Visa, which were based on lists of stolen card data produced by Verizon and Target.[52] Moreover, Target issued public statements announcing the Breach on December 19, 2013, December 27, 2013, and January 10, 2014, and increased the disclosed scope and severity of the Breach with each statement.[53] The Breach was a high visibility event that exposed the Class to massive losses.

Even though the Breach occurred due to !"#$%&'(failings and deficiencies in cybersecurity, Plaintiffs and the Class were forced to bear the financial impact. As described in the Librock Declaration, card issuing institutions were forced to respond to

---

[50] Ex. E at 021-022.

[51] *See* Ex. EE (MasterCard Settlement Agreement) at 8.1.1.3(e)-(g) (stating +3"(&%#)"#I has accurately determined, by applying the relevant MasterCard Operating Regulations in accordance with 3"(&%#)"#I'(customary practices and :#5@%I-#%(L the maximum amount L"&&#42-&"2*% to the Target 4.&#-(45.L=19T Ex. FF at 970-971 [redacted]

[52] *See* Ex. GG; Ex. HH) (spreadsheets identifying each financial institution that received an alert and the number of its accounts affected by the Breach).

[53] *See* Compl. ¶¶71, 73-74.

information that their card accounts were compromised in the Breach. Financial institutions +H"I both a ***financial self-interest*** and ***regulatory obligation*** to take immediate action upon notification of the Target 2#%"@H=1[54] A financial institution that +8"4*(to act upon notification of a data breach 2%&#"/(1 customer trust, and risks losing customers, being subjected to corrective regulatory action and scrutiny, incurring economic losses, and suffering reputational harm.[55] Class members were obligated to respond to the Breach in order to both comply with stringent federal regulations and to avoid or mitigate economic losses from fraudulent transactions in customer accounts, which may be +25#.% in the first instance by the [card issuing] financial 4.(&4&-&45.C1 after a data breach pursuant to federal regulations.[56] For these reasons, Librock opines that:

> Given the nature of the financial data taken and the breadth of the breach, it would have been reasonable for a [class member] to employ any of the following standard responses:
>
> - The monitoring of customer accounts to prevent fraudulent charges;
> - The cancellation or reissuance of any credit or debit cards affected by the breach;
> - The closure of any account affected by the breach and any action to block transactions with respect to affected accounts;
> - The opening or reopening of any accounts affected by the breach;

[54] Librock Decl. at ¶12.

[55] *Id*. at ¶¶11-12.

[56] *Id*. at ¶¶14-15.

- Payment of any refund to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and
- Notification of cardholders affected by the breach.[57]

These responses are consistent with financial institution responses to payment card data breaches that have been specifically recognized by the Minnesota Legislature as appropriate. *See* Minn. Stat. § 325E.64, subd. 3 (PCSA allows recovery for, among other things, cancellation or reissuance of cards, closing or opening of accounts, refund of fraudulent charges and notification of cardholders); *see also In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1313 (D. Minn. 2014) 6!"#$%&'(+I"&" retention practices are governed by the 07)EFM19=

Consistent with ?42#5@A'(opinion, and as discussed in the Cantor Report, Class members did in fact respond to the Target Breach in directionally consistent ways by, *inter alia*, cancelling and reissuing cards, refunding customers for fraudulent transactions, notifying customers, and monitoring for fraud.[58] *See also* Minn. Stat. § 325E.64, subd. 3. !"#$%&'(common actions caused financial institutions to incur common types of costs from the Breach.[59] Dr. Cantor has opined that sufficient data exist for her accurately to calculate class 0%02%#(' damages for fraud losses and reissue costs on an aggregate basis.[60] Like Class members, Target itself received an alert from its card network

[57] *Id.* at ¶21.

[58] Cantor Report at ¶19.

[59] Cantor Report at ¶¶35-49, 51.

[60] Cantor Report at ¶52, 57, 77, 100-101.

regarding Target-issued cards compromised in the Breach.[61] Similar to the Class, Target also reissued its compromised payment cards and was responsible for fraud losses after the Breach of nearly $50,000 ***per day***.[62]

H. The Proposed Class Representatives

Plaintiffs and proposed class representatives Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain are all card-issuing institutions that learned of the Breach alongside all other Class members and were similarly forced to respond to it. In particular:

- Plaintiff Umpqua Bank is a bank with total assets of $22 billion that issued approximately 21,596 Visa branded payment cards that were compromised in the Breach;[63]
- Plaintiff Mutual Bank is a bank with total assets of $454 million that issued approximately 1,391 Visa branded payment cards that were compromised in the Breach;[64]
- Plaintiff Village Bank is a bank with total assets of $190 million that issued approximately 970 Visa branded payment cards that were compromised in the Breach;[65]
- Plaintiff CSE Federal Credit Union is a credit union with total assets of $292 million that issued approximately 445 Visa branded payment cards that were compromised in the Breach;[66] and

---

[61] Ex. II (Bach Dep.) at 6:1-6; 23:8-27:1.

[62] *Id*. at 40:21-23; 59:24-62:10; 76:13-23;112:17-113:9.

[63] Fullerton Decl. ¶¶2, 4, 9. At the time of the Target Breach, Umpqua Bank had an impending merger with Sterling Savings Bank and the two financial institutions have since merged. The total number of cards compromised in the Breach consists of payment cards issued by both Umpqua Bank and Sterling Savings Bank. *Id*. at ¶¶4, 6, 9.

[64] White Decl. ¶¶4, 7.

[65] Diers Decl. ¶¶4, 7.

- Plaintiff First Federal Savings of Lorain is a bank with total assets of $425 million that issued approximately 490 Visa branded payment cards that were compromised in the Breach.[67]

Each of the Plaintiffs received alerts that cards they had issued were compromised in the Breach[68] and responded by, *inter alia*: (i) cancelling compromised cards; (ii) issuing replacement cards; and (iii) absorbing fraudulent charges.[69] 7*"4.&488(' responses are consistent with the responses that card issuing institutions were compelled to, and did in fact take, in response to the Breach,[70] are recognized as reasonable by the PCSA,[71] and taken by Target with respect to its compromised Company-branded cards.[72]

III. ARGUMENT

A. Legal Standards

Federal courts have +2#5"I discretion in determining whether or not to certify a class under Rule UV=1 *Lockwood Motors, Inc. v. Gen. Motors Corp.*, 162 F.R.D. 569, 573

---

[66] Yelverton Decl. ¶¶4, 7.

[67] Brosky Decl. ¶¶4, 7.

[68] Fullerton Decl. ¶¶3, 8; White Decl. ¶5; Diers Decl. ¶5; Yelverton Decl. ¶5; Brosky Decl. ¶5.

[69] Fullerton Decl. ¶5; White Decl. ¶9; Diers Decl. ¶9; Yelverton Decl. ¶9; Brosky Decl. ¶9. Sterling Savings Bank also received notification through CAMS alerts that payment cards it issued had been compromised in the Target Breach. In response, Sterling Savings Bank, *inter alia*, cancelled and reissued cards experiencing fraudulent activity and refunded customers for fraudulent charges. Fullerton Decl. ¶¶8 & 10.

[70] Librock Decl. at ¶21; Cantor Report at ¶43-16.

[71] Minn. Stat. § 325E.64, subd. 3.

[72] Ex. II at 40:21-23; 60:21-23; 61:17-62:10; 76:13-23;112:17-113:9.

(D. Minn. 1995). +WH%. a question arises as to whether certification is appropriate, the court should give the benefit of the doubt to approving the @*"((=1 *Karsjens v. Jesson*, 283 F.R.D. 514, 517 (D. Minn. 2012).

Merits disputes should not be resolved at the class certification stage even if Rule 23's criteria present issues that overlap with merits questions. *In re Zurn Pex Plumbing Prods. Liab. Litig.*, 644 F.3d 604, 617 (8th Cir. 2011). Indeed, +XH%. considering a motion for class certification, a court need not ask whether the plaintiff or plaintiffs have stated a cause of action or will ultimately prevail on the merits, but rather whether the requirements of Rule 23 are 0%&=1 *Karsjens*, 283 F.R.D. at 517. Certification of a class requires meeting the numerosity, commonality, typicality, and adequacy elements of Rule 23(a) and one of the three provisions of Rule 23(b). *See* Fed. R. Civ. P. 23. Plaintiffs move to certify a damages class under Rule 23(b)(3), which requires that +Y-%(&45.(of law or fact common to class members predominate over any questions affecting only individual 0%02%#(C1 and that +" class action is superior to other available methods for fairly and efficiently adjudicating the @5.&#5Z%#(/=1 *Id.*[73]

B. The Class Is Ascertainable

Courts in this Circuit have recognized an +40:*4@4& #%Y-4#%0%.&1 of Rule 23 that +&H% Q@*"((C as proposed, is objectively ascertainable.'1 *Ebert v. Gen. Mills, Inc.*, No. 13-3341 (DWF/JJK)) 2015 WL 867994, at *12 (D. Minn. Feb. 27, 2015). Ascertainability is

[73] In the alternative, Plaintiffs move for certification, under Rule 23(c)(4), of any element of Plaintiffs' claims (such as liability) that the Court finds appropriate for class treatment, if the Court determines that another element is not.

not +" particularly stringent &%(&=1 *Eastwood v. S. Farm Bureau Cas. Ins. Co.*, 291 F.R.D. 273, 278 (W.D. Ark. 2013) (class ascertainable if the +$%.%#"* outlines of the membership of the class are determinable at the outset of the *4&4$"&45.=19= Rather, +"& a minimum, the [class] description must be sufficiently definite that it is administratively feasible for the court to determine whether a particular individual is a 0%02%#=1 *Ebert*, 2015 WL 867994, at *12; *see also Gardner v. Equifax Info. Servs., LLC*, No. 06-3102 (ADM/AJB) 2007 WL 2261688, at *3 (D. Minn. Aug. 6, 2007) (ascertainability is established when class membership can be determined objectively). Plaintiffs move to certify a class of all entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by Target on December 19, 2013.

This Court can easily ascertain who is in the Class based on the objective criteria in the Class definition. Business records identify every Class member in this case. !"#$%&'(own records, information from Verizon and the alerts and records of card brands, including Visa and MasterCard, will demonstrate precisely which 4.(&4&-&45.(' accounts were compromised in the Breach.[74] Thus, Class members are not only ascertainable, they are individually identifiable.

[74] *See* Ex. E at 15; Ex. JJ; Ex. GG; Ex. HH; Ex. KK; Ex. LL; Ex. MM; *see also* Fullerton Decl. ¶¶3, 8; White Decl. ¶5; Diers Decl. ¶5; Yelverton Decl. ¶5; Brosky Decl. ¶5 (financial institutions learned of the Breach from, among other things, alerts from card brands).

C. Rule 23(a) Is Satisfied

1. Numerosity

+O!MH% number of persons in the proposed @*"((1 is the central focus of the numerosity analysis. *Paxton v. Union Nat l Bank*, 688 F.2d 552, 559 (8th Cir. 1982). +N. general, a putative class with over forty members meets this #%Y-4#%O%.&=1 *Ebert*, 2015 WL 867994, at *9; *see also Alberts v. Nash Finch Co.*, 245 F.R.D. 399, 409 (D. Minn. 2007) 6+" putative class exceeding 40 members is sufficiently large to make joinder 4O:#"@&4@"2*%=19=

The Breach affected approximately 40 million payment cards issued by thousands of financial institutions. This is verifiable based on the thousands of unique bank identification numbers 6+GN<19 numbers affected by the Breach, reflected on, *inter alia*, alerts from Card Brands to issuing banks.[75] Numerosity is satisfied.

2. Commonality

Rule 23(a)(2) requires the existence of +Yuestions of law ***or*** fact common to the @*"((C1 and that a class action will +$%.%#"&% common answers apt to drive the resolution of the *4&4$"&45.=1 *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011); *see also In re Lutheran Bhd. Variable Ins. Prods. Co. Sales Practices Litig.*, No. 99DMDD 1309(PAM/JGL), 2004 WL 909741, at *1 (D. Minn. April 28, 2004) (Magnuson, J.). A common question is one +85# which a prima facie case can be established through common %Z4I%.@%=1 *Zurn*, 644 F.3d at 618. However, Rule 23 does not require that all

[75] *See* Ex. GG; Ex. HH; *see also* Ex. KK & Ex. LL (listing over 3,600 financial institutions).

questions are common; +O#M"&H%#C the Rule requires only that common questions %K4(&=1 *Figas v. Wells Fargo & Co.*, No. 08-4546, 2010 WL 2943155, at *4 (D. Minn. Apr. 6, 2010) (Magnuson, J.); *see also Khoday v. Symantec Corp.*, No. 11-180, 2014 WL 1281600, at *15 (D. Minn. Mar. 13, 2014) (noting that +(4.$*% common @5.&%.&45.1 could satisfy commonality). Here, numerous common questions of law and fact will dictate Target's liability to all Class members alike.

Specifically, Plaintiffs' negligence claims based on Target's failure to secure customer payment information will turn factually on the actions Target took or did not take, and whether that conduct enabled the Breach to occur. Legally, negligence claims will depend on whether Target owed a duty to card issuing banks with respect to data security, and whether it was reasonably foreseeable that Target's card data security failures would result in harm to card issuing banks.

Likewise, whether Target's conduct violated the PCSA will be determined by common evidence, including whether Target retained payment card data and whether Target's computer system was breached. None of Targe&'(conduct that resulted in the Breach or violated the PCSA was different as to any particular Class member. Commonality is met.

3. Typicality

Typicality is satisfied when +&H% claims of the named plaintiffs *emanate from the same legal theory* as the claims of the class 0%02%#(=1 *Dirks v. Clayton Brokerage Co. of St. Louis, Inc.*, 105 F.R.D. 125, 133 (D. Minn. 1985); *see also Paxton*, 688 F.2d at 561-62 (typicality established +48 the claims or defenses of the representatives and the

members of the class *stem from a single event* or are *based on the same legal or remedial theory* (quoting C. Wright & A. Miller, *Fed. Prac. & Proc.* § 1764 n. 21.1 (Supp. 1982))). +!H% test for typicality is 0*fairly easily met* so long as other class members have claims similar to the named plaintiff.'1 *Ebert*, 2015 WL 867994, at *9. Moreover, +O&M/:icality is closely related to commonality as a finding of one generally compels a finding of the 5&H%#=1 *In re Select Comfort Corp. Sec. Litig.*, 202 F.R.D. 598, 604 (D. Minn. 2001).

Importantly, +O:M%#8%@& identity of claims is not #%Y-4#%I1 for typicality to be established, and the +:#%(%.@% of differing legal inquiries and factual discrepancies will not preclude class @%#&484@"&45.=1 *Figas*, 2010 WL 2943155, at *4; *see also Smith v. United Health Care Servs., Inc.,* No. 00-1163, 2002 WL 192565, at **3-4 (D. Minn. 2002) (plaintiffs typical of class despite varying degree of damages due to +(&#5.$ similarity of legal &H%5#4%(19=

7*"4.&488(' claims are typical of the)*"((('(= The Class consists of thousands of institutions that issued payment cards that were compromised by Target in the Breach. Plaintiffs and the Class received information regarding !"#$%&'(+H4$H*/ Z4(42*%1 Breach through various outlets including public statements issued by Target on December 19 and 27, 2013, and the alerts from card brands and networks.[76] Once on notice of the Breach, Plaintiffs and the Class were obligated to pursue an active response in order to protect

[76] *See* Compl., ¶¶60, 71, 73; Cantor Report ¶ 44, Exs. 5-6; *see also* Fullerton Decl. ¶¶3, 8; White Decl. ¶5; Diers Decl. ¶5; Yelverton Decl. ¶5; Brosky Decl. ¶5.

their customers from fraud and also to limit liability resulting from fraudulent transactions D costs directly absorbed by the Class and triggered by the Breach.[77] As explained by Librock, +02M".A(were required by regulation to respond in a timely manner to the risks posed by the Target G#%"@H=1[78] Moreover, the Class engaged in common categories of reasonable responses, such as monitoring accounts, cancelling and reissuing compromised cards, notifying customers of the Breach, and refunding customers for unauthorized transactions.[79] 7*"4.&488(' responses to the Breach were virtually identical to other Class members.[80] Typicality is established.

The court in *TJX* determined that the :*"4.&488(' claims were typical of absent class O%O2%#(' because they commonly depended on the O%#@H".&'(conduct:

> It is obvious that the proposed class . . . is premised on the same course of conduct D namely, the alleged failure of [Defendants] to maintain proper data security. . . . Because of these essential similarities between the proposed representatives and a large number of the members of the proposed class . . . the named plaintiffs are typical.

In re TJX Cos. Retail Sec. Breach Litig., 246 F.R.D. 389, 393 & n.4 (D. Mass. 2007).[81] A similar finding is even more appropriate here, where the PCSA identifies specific data breach responses as reasonable. *See* Minn. Stat. § 325E.64, subd. 3.

---

[77] *See* Cantor Report at ¶¶ 35-42, 46; Librock Decl. at ¶12.

[78] Librock Decl. at ¶13; *see also id.* at ¶21.

[79] *See id.*; Cantor Report at ¶ 51.

[80] *See* Parts II.G. & II.H., *supra*.

[81] The *TJX* court ultimately denied certification because :*"4.&488(' theory was based on misrepresentation, which necessarily involved individualized questions of *reliance*.

4. Adequacy

Adequacy is established if 7*"4.&488(' +@5-.(%* is competent to pursue the "@&45.1 and 7*"4.&488(' +4.&%#%(&(are not antagonistic to the interests of the @*"((=1 *In re Monosodium Glutamate Antitrust Litig.*, 205 F.R.D. 229, 233 (D. Minn. 2001) (Magnuson, J.). Here, 7*"4.&488(' interests align with absent Class members as their claims stem from a single course of conduct by Target, are based upon the same legal theories, and seek to recover similar damages for Target's legal violations.

Nothing suggests that Plaintiffs have interests contrary to those of the Class. Rather, Plaintiffs have been actively engaged in prosecuting this case and are committed to monitoring and steering it on behalf of the Class. Furthermore, Plaintiffs have collected and produced documents, responded to written discovery and appeared for 30(b)(6) depositions.[82] Moreover, Plaintiffs have retained and overseen Lead Counsel, whose qualifications the Court has previously recognized and who have conducted this hotly contested litigation.[83] The adequacy requirement is satisfied.

Here, !"#$%&'(liability depends on !"#$%&'(conduct and no claim remaining before the Court requires proving reliance. *See generally In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1312 (D. Minn. 2014) (dismissing claims for negligent misrepresentation and noting that +!"#$%& contends that Plaintiffs have failed to plead any reliance on the alleged 504((45.(19=

[82] *See* Fullerton Decl. ¶¶12-14; White Decl. ¶¶11-14; Diers Decl. ¶¶11-14; Yelverton Decl. ¶¶11-14; Brosky Decl. ¶¶11-14.

[83] *See* ECF Nos. 64; 436 (reappointing Lead and Liaison Counsel and noting that +!H% Court is satisfied that all appointed counsel have faithfully discharged their I-&4%(19T *see also* ECF No. 74 (accepting recommendations for appointments to the executive and steering committees).

D. The Class Satisfies Rule 23(b)(3)

Plaintiffs seeking to certify a damages class must satisfy the requirements of Rule 23(b)(3) by demonstrating that: (1) common questions of law or fact predominate over any questions affecting only individual members 6+:#%I504."@%19; and (2) a class action is superior to other available methods for fairly and efficiently adjudicating the controversy 6+(-:%#45#4&/19= This Class meets both prerequisites.

1. Common Issues of Fact and Law Predominate.

Predominance +&%(&(whether proposed classes are sufficiently cohesive to warrant adjudication by #%:#%(%.&"&45.=1 *AmChem Prods., Inc. v. Windsor,* 521 U.S. 591, 623 (1997). +!H% predominance inquiry requires an analysis of whether a prima facie showing of liability can be proved by common evidence or whether this showing varies from member to 0%02%#=1 *Halvorson v. Auto–Owners Ins. Co.,* 718 F.3d 773, 778 (8th Cir. 2013). +G%@"-(% no precise test can determine whether common issues predominate, the Court must pragmatically assess the entire action and the issues 4.Z5*Z%I=1 *Khoday*, 2014 WL 1281600, at *18. The central issue is whether I%8%.I".&'(liability as to all plaintiffs can be established by common evidence. *Avritt v. Reliastar Life Ins. Co.,* 615 F.3d 1023, 1029 (8th Cir. 2010). Here, common issues predominate, as the essential elements of all of Plaintiffs' common legal theories can be established through common evidence, and Minnesota law applies to all claims.

(a) Minnesota Law Should Apply to the Claims of All Class Members

+0,M%I%#"* courts sitting in diversity apply the forum state's conflict of laws #-*%(=1 *Nesladek v. Ford Motor Co.*, 46 F.3d 734, 736 (8th Cir. 1995) (citing *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941)). An MDL court must apply the choice-of-law rules of the state in which the action was filed. *Ferens v. John Deere Co.*, 494 U.S. 516, 524 (1990). Because this Court sits in diversity and because all class-representative Plaintiffs filed their actions in Minnesota, the Court should apply Minnesota's choice-of-law rules. *See* Compl. ¶4 (pleading diversity jurisdiction and compliance with Class Action Fairness Act).

As demonstrated below, 34..%(5&"'(statutory and common law should govern the claims of all Class members. This Court has already determined that the PCSA applies to losses incurred by entities outside Minnesota based on !"#$%&'(violation of that act. *Target*, 64 F. Supp. 3d at 1313. Furthermore, 34..%(5&"'(choice-of-law rules favor application of Minnesota negligence and negligence per se law (and to the extent necessary, the PCSA) given the overwhelming factual connections each Class member's claim has to !"#$%&'(conduct in Minnesota.

(i) The PCSA expressly directs application of Minnesota statutory law in this case

A state may enact a choice-of-law rule legislatively, as applicable to a particular issue of law. This is referred to as legislative jurisdiction, and such a rule operates irrespective of interstate conflicts of law, and subject only to the limitations of the Due Process and Full Faith and Credit clauses of the U.S. Constitution. *McCluney v. Jos.*

Schlitz Brewing Co., 649 F.2d 578, 580-581 and n.3 (8th Cir. 1981) "88'IC 454 U.S. 1071 (1981); *see also Target*, 64 F. Supp. 3d at 1313.

When the Minnesota legislature prescribes a right to be vindicated in state-specific terms, it intends that the statute apply to all claims that meet the Minnesota-specific criteria. *See Bozied v. Edgerton*, 58 N.W.2d 313, 315 (Minn. 1953) (holding that statute permitting general recovery in context of +2-(4.%((transacted, in whole or in part, ***within the state [of Minnesota]***C1 applied to non-resident injured by Minnesota purchaser, and stating, +?4A% any other statute phrased in words of general application, its protective coverage [in the absence of an expression of legislative intent to the contrary [is not limited to residents of the (&"&%=19T *Renlund v. Commodore Mining Co*., 93 N.W. 1057, 1059 (Minn. 1903) (statute generally permitting recovery by dependents suffering a loss +#%(-*&4.$ from an act of negligence committed ***within the state [of Minnesota]***1 was applicable to claims by out-of-state persons in the absence of +" word or expression indicating an intention to limit its application to persons residing within the (&"&%19= That is precisely what Minnesota did by including a Minnesota-specific jurisdictional hook within the PCSA.[84]

[84] The PCSA and the statutes at issue in *Bozied* and *Renlund* are distinguishable from the Private Attorney General Act at issue in *In re St. Jude Medical, Inc*., 425 F.3d 1116 (8th Cir. 2005). The Act at issue in *St. Jude* contained no jurisdictional hook expressing the intent that the consumer statutes should apply when an entity doing business *in Minnesota* is alleged to have violated the statute. The Minnesota Supreme Court in *Bozied* and *Renlund* made clear that when a statute creating a general right of action contains a Minnesota jurisdictional hook related to liability, it must be applied to non-residents unless it ***expressly limits*** application to residents.

The PCSA contains the choice-of-law rule applicable to claims under it. This Court has already recognized that the PCSA applies to any person or entity conducting business in Minnesota, and thus flatly rejected Target's contention that the PCSA covers only business transactions that take place in Minnesota:

> The Act does not apply only to business transactions that take place in Minnesota. By its terms, it applies to the data retention practices of any person or entity +@5.I-@&4.$ business in 34..%(5&"=1 Minn. Stat. § 325E.64, subd. 2. Target is a Minnesota company that conducts business in Minnesota, and thus its data retention practices are governed by the Act. And contrary to Target's assertions, the application of the PCSA to out-of-state transactions does not implicate the dormant Commerce Clause.

Target, 64 F. Supp. 3d at 1313. Because +O&H% PCSA] applies equally to the Minnesota companies' data retention practices with respect to in-state and out-of-state &#".("@&45.(C1 it applies to the claims of all Class members (the issuers of cards compromised as a consequence of those transactions) against Target here. *Id*. The provision, +@5.I-@&4.$ business in Mi..%(5&"C1 directs Minnesota courts to apply the PCSA when the Minnesota-specific criterion is met. Minn. Stat. § 325E.64, subd. 2. This choice-of-law rule is subject only to the federal C5.(&4&-&45.'(limitations on Minne(5&"'(legislative jurisdiction.

(ii) Each Class member's claims has significant contacts with Minnesota

The Supreme Court has described the constitutional restrictions of the application of forum law as +05I%(&=1 *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 818 (1985). +,5# a State's ***substantive law*** to be selected in a constitutionally permissible manner, that State must have a significant contact or significant aggregation of contacts, creating

state interests, such that choice of its law is neither arbitrary nor fundamentally -.8"4#=1 *Jepson v. Gen. Cas. Co. of Wis.*, 513 N.W.2d 467, 469 (Minn. 1994). The Court must satisfy itself that Minnesota has sufficient contacts +X4&H each plaintiff class member's @*"4O=1 *St. Jude*, 425 F.3d at 1120. Each Class 0%02%#'(claim has significant contacts with Minnesota such that application of Minnesota law satisfies the Due Process and Full Faith and Credit clauses of the U.S. Constitution.

Target is incorporated and headquartered in Minnesota, and Target maintains its relevant servers within the state.[85] Discovery developed to date establishes !"#$%&'(negligence and failure to properly safeguard financial data prior to and during the Breach by ignoring alerts that malware had been detected on its servers in Minnesota. The malware retained all the POS-scraped data on !"#$%&'(servers in Minnesota. That data was gathered on and exfiltrated from servers in Minnesota.[86] Furthermore, !"#$%&'(negligence, including its failure to heed specific warnings from its own employees about security vulnerabilities, its failure to hire employees competent to manage security systems and protocols, its disregard of repeated alerts from security providers, and its decisions to disable security features on its antivirus and malware prevention providers D occurred or emanated from decisions made in Minnesota.[87] All of these contacts apply equally to each class member and to the PCSA and negligence claims, and accordingly,

[85] Compl. ¶13; Answer ¶13; Ex. W at 66:6-21; 162:24-163:1.

[86] Ex. W at 66:6-21; 162:24-163:1; Ex. S at -425-426; *see also* Part II, *supra*.

[87] Ex. W at 180:10-17; 160:3-4; Ex. D at. 210:10-12; Ex. A. 268:5-8; *see also* Part II, *supra*.

Minnesota law may be constitutionally applied. *See Mooney v. Allianz Life Ins. Co. of N. Am.*, 244 F.R.D. 531, 535 (D. Minn. 2007) (holding that the +@5.&"@&([including that defendant is incorporated and headquartered in Minnesota and that the allegedly fraudulent marketing materials were prepared and distributed from Minnesota] are sufficient to allow application of Minnesota law to the claims of non-Minnesota class members without offending either the Due Process Clause or the Full Faith and Credit)*"-(%19=

(iii) Minnesota's negligence law should apply

While the choice-of-law directive of the PCSA is clear, it is equally clear that Minnesota law applies to all Class 0%02%#(' negligence-based claims. Minnesota's generally applicable choice-of-law rules dictate that when a conflict arises, a court must first decide whether the conflict involves substantive law, as opposed to procedural or remedial law. *Schumacher v. Schumacher*, 676 N.W.2d 685, 690 (Minn. Ct. App. 2004); *Davis v. Furlong*, 328 N.W.2d 150, 153 (Minn. 1983) (matters of procedure and remedies are governed by law of forum); *Schwan s Sales Enters., Inc. v. SIG Pack, Inc.*, 476 F.3d 594, 596 (8th Cir. 2007) (same). +0EM-2(&".&4Z% law is that part of the law which creates, defines, and regulates rights,1 *Schumacher*, 676 N.W.2d at 690, and +I4#%@&*/ impacts on the accrual of a cause of action in the first 4.(&".@%=1 *Ferris, Baker Watts, Inc. v. Deutsche Bank Sec. Ltd.,* Nos. 02-3682, 02-4845, 2004 WL 2501563, *4 (D. Minn. 2004).

Once a true conflict of substantive law is established, the court must then analyze the following factors to determine which (&"&%'(law should apply: +6\9 predictability of

result; (2) maintenance of interstate and international order; (3) simplification of the judicial task; (4) advancement of the forum's governmental interest; and (5) application of the better rule of *"X=1[88] *Jepson*, 513 N.W.2d at 470 (citing *Milkovich v. Saari,* 203 N.W.2d 408, 412 (Minn. 1973)).

Assuming, *arguendo*, that there are at least some substantive conflicts between Minnesota law and the law of some other states regarding the accrual of Plaintiffs' negligence claims, 34..%(5&"'(choice-of-law factors clearly favor the application of Minnesota law in this case. *See Mooney*, 244 F.R.D. at 534 6+G%@"-(% of the outcome of the choice-of-law analysis below, it is unnecessary to determine the precise number of outcome-determinative @5.8*4@&(1 in issue). Furthermore, even if the Court must analyze the PCSA claim under the *Milkovich* factors, those factors favor application of the PCSA to all Class 0%02%#(' claims.

(1) Predictability of results

The first factor addresses +XH%&H%# the choice of law was predictable before the time of the transaction or event giving rise to the cause of "@&45.=1 *Danielson v. Nat l Supply Co.*, 670 N.W.2d 1, 7 (Minn. Ct. App. 2003). +!5#& actions generally do not implicate party expectations because torts stem from unplanned "@@4I%.&(=1 *Lommen v.*

[88] The +2%&&%# rule of *"X1 factor has been given +Q.5 significant X%4$H&' by the Minnesota Supreme)5-#&=1 *Lutheran Ass n of Missionaries and Pilots, Inc. v. Lutheran Ass n of Missionaries and Pilots, Inc.*, No. 03-6173, 2004 WL 1212083, at *3 (D. Minn. May 20, 2004) (Magnuson, J.). Nonetheless, this factor would weigh in favor of Minnesota law, because Minnesota has, in the form of the PCSA, a uniquely developed policy and mechanism providing recourse for card-issuing financial institutions harmed by the security breach of a merchant.

City of E. Grand Forks, 522 N.W.2d 148, 150 (Minn. Ct. App. 1994). Here, however, it is predictable that Minnesota law would govern !"#$%&'(liability for a massive data breach rooted in Minnesota. Target and financial institutions could fairly expect Minnesota law to apply to issues relating to Target's handling of payment card data because of (1) the PCSA, (2) !"#$%&'(status as a Minnesota corporation, headquartered within this state, and (3) the idiosynctraic centralization of systems in Minnesota whose breach caused harm nationwide in one fell swoop. The factual underpinnings of all the legal theories also make Minnesota law the most predictably applicable. The +#%&%.&45.1 of data predictably occurred in Minnesota. !"#$%&'(duty arose from data protection systems maintained, and protocols followed or ignored, in Minnesota.[89] Target breached its duty in Minnesota. Its breach of duty caused common impact across the Class by exposing protected financial data from servers in Minnesota. Further, Target's failures D to prevent the breach and to secure protected information D occurred in Minnesota.[90] *See Mooney*, 244 F.R.D. at 536 (holding that defendant +@5-*I have predicted that Minnesota law would govern claims based on [defendant's] allegedly fraudulent activities that emanated from 34..%(5&"19= Accordingly, this factor favors the application of Minnesota law to each Class 0%02%#'(claim.

[89] *See* Ex. W at 66:6-21; 160:3-4; 162:24-163:1; 180:10-17; Ex. D at 210:10-12; Ex. A. 268:5-8.

[90] *See* Ex. W at 72:8-74:21; 76:1-5; Ex. S at 425-426.

(2) Maintenance of interstate and international order

+!H4(factor requires that the states whose laws are applied have sufficient contacts with the facts in 4((-%=1 *Fee v. Great Bear Lodge of Wis. Dells, LLC*, No. 03-3502, 2004 WL 898916, at *2 (D. Minn. Apr. 9, 2014) (Magunson, J.). As set forth above, Minnesota has more substantial contacts to each Class member's claims and the underlying facts than even non-Minnesotan Class 0%02%#(' resident jurisdictions.[91] *Mooney*, 244 F.R.D. at 536 (finding that the application of Minnesota law is supported by this factor because +0I%8%.I".&M is a Minnesota corporation that allegedly created fraudulent marketing materials in Minnesota, distributed them from Minnesota, and benefitted from [them] . . . when it received [payments] in 34..%(5&"19= As such, this factor weighs in favor of applying Minnesota law.

(3) Simplification of the judicial task

+!H% third factor, simplification of the judicial task, has not been given much X%4$H&1 by the Minnesota Supreme Court. *Nodak Mut. Ins. Co. v. Am. Family Mut. Ins. Co.*, 604 N.W.2d 91, 95 (Minn. 2000). Of course, +4& would be simpler to apply the law of one state than the law of multiple (&"&%(=1 *Mooney*, 244 F.R.D. at 536. But this Court is capable of resolving +.5.-Minnesota class member's claims under Minnesota law or the law of the non-resident's home (&"&%=1 *Id.* This factor is then, at worst, neutral to the application of Minnesota law.

---

[91] *See supra,* at 31-32 (discussing !"#$%&'(and the G#%"@H'(ties to Minnesota).

(4) Advancement of the forum's governmental interest

+Under the fourth factor, the Court must weigh the policy interests of Minnesota with those of a non-Minnesota class 0%02%#'(home (&"&%=1 *Mooney*, 244 F.R.D. at 536-537. +!H4(factor is designed to assure that Minnesota courts do not have to apply rules of law that are inconsistent with 34..%(5&"'(concept of fairness and %Y-4&/=1 *Lutheran Ass n*, 2004 WL 1212083, at *3. The Minnesota legislature has codified an unequivocal policy, which provides that card issuing financial institutions that have been harmed by a security breach may seek redress from the merchant that experienced the breach. This policy is embodied in the PCSA, which polices Minnesota corporations by strictly assigning liability to any infringing entity conducting business in Minnesota. *See Mooney*, 244 F.R.D. at 537 (finding that this factor weighed in favor of applying Minnesota law because +&H% Minnesota legislature has evinced a strong policy providing redress for fraudulent business practices that occur within 34..%(5&"'(borders, regardless of where a @5.(-0%#'(injury occurs L [and] [a]lthough other states have an interest in applying their own laws, their interest is not so strong as to prevent their citizens from benefitting from 34..%(5&"'(willingness to provide statutory and common law remedies for fraudulent conduct emanating from 34..%(5&"19= Furthermore, 34..%(5&"'(strong policy interest in deterrence independently extends to tort cases where Minnesota was in essence the source of the harm, as here, where !"#$%&'(security failures in Minnesota were directly responsible for the)*"((('(injuries. *See Fluck v. Jacobson Mach. Works, Inc.*, No. CX-98-1899, 1999 WL 153789, at *3 (Minn. Ct. App.

Mar. 23, 1999) 634..%(5&"'(policy interest of deterring manufacturers from placing a defective product into stream of commerce from within its borders is sufficient to apply Minnesota law to injury that occurred in Colorado). The governmental interest factor favors the application of Minnesota law to all class 0%02%#(' claims and, under the *Milkovich* analysis, Minnesota law applies to all claims and Class members.

(b) Common Questions Predominate as to the PCSA Claims

The PCSA claim is appropriate for class treatment under Rule 23(b)(3) because Plaintiffs will +:#5Z%1 (or Target will disprove) through +$%.%#"*4S%I %Z4I%.@%1 that Target violated the PCSA +5. a class-wide 2"(4(=1 *Buetow v. A.L.S. Enters., Inc.*, 259 F.R.D. 187, 190 (D. Minn. 2009); *see also Target*, 64 F. Supp. 3d at 1313-12 (discussing liability under the PCSA). Target violated the PCSA if it retained specified payment card data beyond the statutorily permitted period. Minn. Stat. § 325E.64, subd. 2; *Target*, 64 F. Supp. 3d at 1313. Target is liable for such violation if there was +" breach of the (%@-#4&/1 of !"#$%&'(+(/(&%0=1 Minn. Stat. § 325E.64, subd. 3. Upon these factual predicates, Target is obligated to +#%402-#(%1 financial institutions for +@5(&(of reasonable actions undertaken L as a result of the 2#%"@H=1 *Id.*

Plaintiffs can establish the 7)EF'(+retention1 element[92] through common evidence of, for example, Target's practice of storing unencrypted payment card information, including the full magnetic stripe data, on POS terminals beyond the sales

[92] The meaning of the term +#%&"4.1 in the PCSA is a question of statutory interpretation and will apply to all class members in the same way. *See e.g. In re Welfare of J.J.P.*, 831 N.W.2d 260, 264 (Minn. 2013) 6+E&"&-&5#/ interpretation is a question of *"X19=

transactions.[93] Moreover, Target had a practice of storing unencrypted payment card information on its servers for years.[94] !"#$%&'(storage of card data from customer transactions is underscored by the Senate Report, which discusses how the breach affected +*areas of Target s network ... storing consumer data*=1[95] Furthermore, Target retained protected card data between November 29 and December 15, 2013, by disabling malware-security functions, ignoring repeated alerts as to the ongoing Breach, and otherwise failing to delete malware that warehoused protected information on its servers for at least six days at a time.[96] These facts pertain to all class members alike.

Moreover, Target's +(/(&%01 was indisputably breached. As a consequence protected information from approximately 40 million payment cards was compromised.[97] According to the Senate Committee on Science, Commerce and Transportation, intruders +$"4.%I access to Target's computer network [and] stole financial and personal information of as many as 110 million Target @-(&50%#(0=M1[98] This evidence of a +2#%"@H1 likewise applies to all Class members.

---

[93] Ex. W at 72:8-74:21; 76:1-76:5.

[94] Ex. E at 021 & -081.

[95] Ex J at i.

[96] Section II.A., *supra*; Ex. S at -425-426.

[97] *See* Ex. E at 028 (Verizon determined that 39,292,617 unique payment cards were deemed at risk).

[98] Ex. J at i; Ex. CC.

Finally, Plaintiffs will establish through common proof that the Breach proximately caused harm to Class members. Class members received information that specific cards they had issued were compromised in the Breach and were forced to respond.[99] In particular, card issuing financial institutions are subject to the Electronic Funds Transfer Act, Truth-in-Lending Act, Gramm-Leach-Bliley Act, FDIC regulatory guidance requiring the development and implementation of written Identity Theft Protection Programs, U.S. Securities and Exchange Commission regulations, and regulation by the Consumer Finance Protection Bureau, and had to take immediate measures to safeguard not only their own financial interests, but also the best interests of their customers.[100] Reasonable (and in some aspects required) responsive actions included canceling and reissuing compromised cards, notifying customers of the breach, and monitoring and refunding customers for fraudulent activity.[101] The actual harm suffered by Class members D incurring the costs of these responses D can be calculated on a class-wide basis, using the formulaic methodology articulated by economist, Dr. Cantor, discussed below.[102] Thus, common questions predominate as to Plaintiffs' PCSA claim.

[99] Librock Decl. at ¶¶10-13; Ex. GG; Ex. HH.

[100] Librock Decl. at ¶¶14-19.

[101] Librock Decl. at ¶21.

[102] Cantor Report at ¶¶ 47-95.

(c) Common Questions Predominate as to the Negligence-based Claims

Each of the four elements of negligence D +6\9 the existence of a duty of care; (2) a breach of that duty; (3) an injury; and (4) the breach of the duty being the proximate cause of the injury,1 *Smith v. United States*, No. 13-3277, 2015 WL 278252, at *7 (D. Minn. Jan. 22, 2015) (quoting *Engler v. Ill. Farmers Ins. Co.,* 706 N.W.2d 764, 767 (Minn. 2005), will be established through common evidence.

With respect to the duty of care, Minnesota law looks to five factors: +6\9 the foreseeability of harm to the plaintiff, (2) the connection between the defendant's conduct and the injury suffered, (3) the moral blame attached to the defendant's conduct, (4) the policy of preventing future harm, and (5) the burden to the defendant and community of imposing a duty to exercise care with resulting liability for 2#%"@H=1 *Fetterly v. Ruan Logistics Corp.*, No. 12-2617, 2013 WL 6175181, at *3 (D. Minn. Nov. 25, 2013) (Magnuson, J.). +!H% duty to exercise reasonable care arises from the probability or foreseeability of injury to the :*"4.&488=1 *Domagala*, 805 N.W.2d 14, 26 (Minn. 2011).

Courts routinely certify negligence theories for class treatment when the harms caused are not based on personal injury, and common issues predominate. *See Zurn*, 644 F.3d at 619-20 (affirming certification of negligent manufacture of plumbing fixture purchaser class); *In re Zurn Pex Plumbing Prods. Liab. Litig.*, 267 F.R.D. 549, 565 (D. Minn. 2010) (same); *Cromeans v. Morgan Keegan & Co.*, 303 F.R.D. 543, 557-58 (W.D. Mo. 2014) (certification of negligent underwriting class); *Smith v. ConocoPhillips Pipe*

Line Co., 298 F.R.D. 575, 586 (E.D. Mo. 2014) (certifying property contamination class). In the present case, common issues of law and fact predominate as to the issues of duty, breach, causation, and the fact of harm.

Discovery has confirmed numerous common facts showing that Target owed a duty of care to Plaintiffs, which Target breached. For example:

- Throughout 2013, Target received numerous warnings regarding malware targeting POS terminals, including the exact malware used to effectuate the Breach D BlackPOS. Target, however, failed to take action sufficient to prevent the incursion.[103]

- Two independent studies were conducted in 2013, which found clear deficiencies in !"#$%&'(cybersecurity system and which made recommendations for its improvement. Target, however, largely ignored the recommendations.[104]

- Target disabled security features on both Symantec, its antivirus software, and FireEye, its malware application. With respect to Symantec, Target kept features disabled through Black Friday. With respect to FireEye, Target only implemented its detection mode and not its prevention feature, which was designed to stop malware from entering !"#$%&'(system.[105]

- Target failed to integrate the FireEye detection mode properly, so alerts were not being monitored. Thus, the malware detection tool was rendered useless.[106]

- Target allowed vendors, like Fazio, direct access to its system, and Target failed to follow its own procedures for vendor security. In particular,

---

[103] Ex. I; Ex. J; Ex. K; Ex. M at 436-447; Ex N; Ex. A at 228:19-229:23; 233:21-234:9; 275:21-278:10.

[104] Ex. NN at -755; Ex. G at 035-038.

[105] Ex. O at 795; Ex. P at 53:4-17; 62:14-63:2; 177:22-178:20; Ex. E at 020 & 023; Ex Z at 342; Ex. X.

[106] Ex. P at 60:19-62:5.

Target failed to conduct a risk assessment of Fazio and failed to employ a two-factor authentication in order for Fazio to log-in, in direct contravention to !"#$%&'(policies.[107]

- Once the Breach began, Target ignored warnings and alerts on November 24, 25, 26, 30 and December 2. !"#$%&'(own employee recognized, based on an alert, that +(50%5.%'(using a service account to access all the registers in one (&5#%0CM1 but Target failed to effectively respond and pushed off responding to alerts in favor of Cyber Monday.[108]

Furthermore, causation will be based on common facts including the information identifying the affected cards and institutions and the Librock Declaration, which identifies discrete actions, consistent with the PCSA, that financial institutions reasonably undertook in response to the Breach.[109] Damages likewise will be determined through a common methodology, as described below. Accordingly, common issues predominate with respect to Plaintiffs' negligence claim. *See*, *e.g.*, *Zurn*, 267 F.R.D. at 565 (holding that common questions predominated on plaintiffs' negligence claims and stating +[t]hat there may be some individualized issues does not outweigh the number, significance, and predominance of the common questions raised H%#%19T *Ebert*, 2015 WL 867994, at *15 (holding that negligence claim based on property contamination satisfied predominance and stating +&H% key issues of fact and law proposed for class treatment can be addressed

[107] Ex. T at 121:9-18; 157:4-9; Ex. U at 85:5-10; 100:8-101:25; 116:7-117:14; 159:19-163:1; 174:1-177:4; Ex. V at 293, 309 & 314.

[108] Ex. E at 020 & 023; *see also generally* Ex. X; Ex. Z; Ex. BB; Ex. Y.

[109] Librock Decl. at ¶21.

through common proof. Although there are a number of individualized issues, they do not :#%I5O4."&%19=[110]

(d) Damages can be calculated on a class-wide basis

+F& class certification, plaintiff must present a likely method for determining class damages, though it is not necessary to show that this method will work with certainty at this &4O%=1 *Khoday*, 2014 WL 1281600, at *32. Accordingly +&H% Court must consider whether Plaintiffs have sufficiently demonstrated that damages are capable of measurement on a class-wide 2"(4(=1 *IBEW Local 98 Pension Fund v. Best Buy Co.*, No. 11-429, 2014 WL 4746195, at *8 (D. Minn. Aug. 6, 2014). Of course, an +"((%((O%.& of the amount of damages . . . may be properly "(@%#&"4.%I1 after class certification. *Blades v. Monsanto Co.*, 400 F.3d 562, 570 (8th Cir. 2005); *see also Brown v. Hain Celestial Group, Inc.*, No. 11-3082, 2014 WL 6483216, at *19 (N.D. Cal. Nov. 18, 2014) (certification under Rule 23 looks to an acceptable class-wide damages approach and not an actual calculation of damages).

Any variation in damages between class members is of no moment. *See, e.g., In re Nexium Antitrust Litig.*, 777 F.3d 9, 21 (1st Cir. 2015) 6+4& is well established that the

[110] Plaintiffs' negligence per se claim will be determined from the same common evidence as the PCSA and negligence claims. The negligence per se elements are: (1) the violation of a statute; (2) causation; and (3) damages. *See Dillard v. Torgerson, Inc.*, No. 05-2334, 2006 WL 2974302, at *4 n.2 (D. Minn. Oct. 16, 2006) (Magnuson, Props., J.). As set forth above: (i) both Target's violation of the PCSA and issues of causation will be established through common evidence; and (ii) damages can be calculated in a class-wide, formulaic manner. Accordingly, common issues predominate with respect to Plaintiffs' negligence per se claim. *See In re Copley Pharm., Inc.*, 158 F.R.D. 485, 492 (D. Wy. 1994) (predominance satisfied for negligence per se claim).

individuation of damages L is rarely determinative under Rule UV6296V919T *Butler v. Sears, Roebuck and Co*., 727 F.3d 796, 801 (7th Cir. 2013) (stating that +&H% fact that damages are not identical across all class members should not preclude class @%#&484@"&45.19T *see also In re Workers Comp*., 130 F.R.D. 99, 108 (D. Minn. 1990) 6+O&MH% mere existence of individual questions such as damages does not automatically preclude satisfaction of the predominance requirement, so long as there is *some common proof* to adequately demonstrate *some damage* to each :*"4.&488=19=

Plaintiffs' damages methodology is specifically designed to calculate financial institution losses directly related to 7*"4.&488(' theories of liability. *See Comcast Corp. v. Behrend*, 133 S. Ct. 1426 (2013). As set forth above, the Librock Declaration identifies certain standard and reasonable responses, consistent with the PCSA, that financial institutions may undertake in the wake of a security breach.[111] Fraud losses and reissue costs can be calculated on a class-wide basis, as set forth in the economic opinion of Dr. Robin Cantor.[112] In particular, Dr. Cantor observed, from common evidence, that: (i) card-issuing financial institutions must affirmatively respond to data breaches such as the Breach in order to comply with their regulatory obligations, economic self-interest and customer needs[113]; (ii) institutions did in fact respond to the Breach in discrete ways[114]; (iii) economic damages from these responses D in the form of reissuance costs and fraud

[111] Librock Decl. at ¶21.

[112] Cantor Report at ¶¶ 47-95.

[113] Cantor Report ¶¶ 35-42.

costs D can accurately be estimated on a class-wide basis from common information through application of an economically sound methodology[115].

The proposed damages methodology relates directly to Class members' claims. The PCSA explicitly provides for the reimbursement of financial institutions for post-data breach reissuance and fraud costs. Minn. Stat. § 325E.64, subd. 3. Similarly, damages under Plaintiffs' negligence and negligence per se theories are intended to place the victim in the position they would have been absent the harm, *Carpenter v. Auto. Club Interinsurance Exch.*, 58 F.3d 1296, 1305 n.4 (8th Cir. 1995) (citing *Restatement (Second) of Torts* § 903 (1977)), meaning that financial institutions should be restored to the position they would have been in had the Breach not occurred. Accordingly, the class-wide damages methodology is consistent with 7*"4.&488(' liability theories, and predominance is further satisfied.

2. Superiority Is Established

Rule 23(b)(3) also requires a plaintiff to show that a class action is +(-:%#45# to other available methods for fairly and efficiently adjudicating the @5.&#5Z%#(/=1 Fed. R. Civ. P. 23(b)(3). Pertinent to the inquiry are the following:

(1) Class 0%02%#(' interests in individually controlling their separate actions;

(2) The extent and nature of existing litigation by class members concerning the same claims;

(3) The desirability of concentrating the litigation in the particular forum; and

---

[114] Id. ¶¶ 43-46.
[115] ID. ¶¶ 47-95.

(4) The likely difficulties in managing a class action.

Fed. R. Civ. P. 23(b)(3).

Here, there is no evidence demonstrating that Class members maintain an interest in individually controlling thousands of separate actions. Likewise, there is minimal existing litigation by Class members concerning similar claims D in particular after this MDL (which gathered the parallel cases that had been filed) was created. And notably, smaller financial institutions, which constitute most of the Class and which naturally issued fewer cards than larger banks, would likely not be able to justify the cost of pursuing their claims individually.

Moreover, all Class members' claims arise out of Target's conduct in Minnesota, and are based on Minnesota law. This Court is thus the appropriate forum for this litigation, as Target insisted when it sought to transfer all cases here. *See* ECF No. 90 at 1 (+!H% District of Minnesota is the superior forum for these cases. Target is headquartered in the district L a majority of witnesses and documents common to all cases are located &H%#%19= Further, Plaintiffs do not foresee significant difficulties in managing this case as a class action, especially because Minnesota law applies to all Class members. Lastly, because the Breach affected thousands of financial institutions located across the United States, resolving this controversy on a class-wide basis will reduce litigation costs for all parties while promoting judicial economy. Target implicitly acknowledged the utility of the class mechanism in this matter through its attempts to

collectively settle the claims of hundreds of class members.[116] Accordingly, superiority is established. *See In re Potash Antitrust Litig.*, 159 F.R.D. 682, 699 (D. Minn. 1995) (superiority satisfied where +0(M%:"#"&% proceedings would produce duplicate efforts, unnecessarily increase the costs of litigation, impose an unwarranted burden on this Court and other courts throughout the country, and create the risk of inconsistent results for similarly situated :"#&4%(1 and pursuing smaller claims +X5-*I not be %@5.504@"*=19=

E. The Court May Alternatively Certify Certain Issues for Class Treatment

While certification of the proposed class under Rule 23(a) and (b)(3) is eminently appropriate, as an alternative, the Court may certify a limited number of liability issues and allow Class members to seek individual recoveries predicated on a common set of liability findings.

,%I%#"* B-*% 58)4Z4* 7#5@%I-#% UV6@96]9 :#5Z4I%(&H"&^ +0XMH%. ":::#5:#4"&%C ". action may be brought or maintained as a class action with respect to particula# 4((-%(=1 The Advisory Committee Notes of 1966 further state:

> This provision recognizes that an action may be maintained as a class action as to particular issues only. For example, in a fraud or similar case &H% "@&45. 0"/ #%&"4. 4&(+@*"((1 @H"#"@&%# 5nly through the adjudication of liability to the class; the members of the class may thereafter be required to come in individually and prove the amounts of their respective claims.

Fed R. Civ. P. 23 Advisory Committee Notes (1966). A matter is appropriat% 85# +4((-% @%#&484@"&45.1 XH%#% (-@H @%#&484@"&45. X5-*I 4.@#%"(% &H% %884@4%.@/ 58 &H% *4&4$"&45.= *See*

[116] Ex. EE.

St. Jude Med., Inc. v. AARP, 522 F.3d 836, 841 (8th Cir. 2008). Here, all issues related to !"#$%&'(*4"24*4&/ "#% I%:%.I%.&5. @5005. %Z4I%.@%= !H%(%*4"24*4&/ 4((-%(4.@*-I%^[117]

PCSA

- Whether Target retained protected card information in violation of the PCSA;
- WH%&H%# &H% G#%"@H @5.(&4&-&%I " +2#%"@H1 58 0!"#$%&'(M system under the PCSA; and
- Whether the Breach proximately caused harm to the Class.

Negligence

- Whether Target owed a duty to protect the Class from the Breach;
- Whether Target breach its duty to the Class through its action and inaction that allowed the Breach to occur; and
- WH%&H%# &H% 2#%"@H 58 !"#$%&'(I-&/ @"-(%I H"#0 &5 the Class.

As set forth above, while damages for 7*"4.&488(' theories of liability are measurable on a common class-wide basis and likewise depend on common evidence, certification of the foregoing liability issues, at a minimum, will increase judicial efficiency, leaving only remaining issues to be resolved individually. *See Sondel v. N.W. Airlines, Inc.*, No. 3-92-381, 1993 WL 559031, at *11 (D. Minn. Sept. 30, 1993) (holding that +B-*% 23(c)(4) allows the district court to certify a class as to one or more claims without certifying the entire @50:*"4.&19T *Schneider v. United States*, No. 99-0315, 2000 U.S. Dist. LEXIS 19823, at *26 (D. Neb. Mar. 24, 2000) (finding that the certification of a class consisting of Nebraska landholders for the purpose of determining whether and under what circumstances an unconstitutional taking occurred is appropriate under Rule 23(c)(4)); *Charron v. Pinnacle Group N.Y., LLC*, 269 F.R.D. 221, 239, 244 (S.D.N.Y.

[117] !"#$%&'(liability to the Class for negligence per se will rest on the same factual findings that determine 7*"4.&488(' PCSA and negligence claims. *See supra* n.111.

2010) (certifying +" (b)(3) class, limited to certain common liability issues pursuant to B-*%UV6@96]91 and noting that +4. the event J%8%.I".&(' alleged scheme is found to have violated RICO and/or the NYCPA, the Court will consider its options for resolving individual damages 4((-%(=19=

F. Rule 23(g) Appointment of Class Counsel is Warranted

+F court that certifies a class must appoint class @5-.(%*=1 Fed. R. Civ. P. 23(g). In appointing class counsel, the court must consider: +649 the work counsel has done in identifying or investigating potential claims in the action; (ii) @5-.(%*'(experience in handling class actions, other complex litigation, and the types of claims asserted in the action; (iii) @5-.(%*'s knowledge of the applicable law; and (iv) the resources that counsel will commit to representing the @*"((=1 Fed. R. Civ. P. 23(g)(1). Defendant does not oppose the adequacy of the proposed Co-Lead Counsel and Co-Class Counsel for purposes of Federal Rule of Civil Procedure 23(g)(1) and (4).[118]

Plaintiffs propose Chestnut Cambronne and Zimmerman Reed as Co-Lead Class Counsel, and the firms of Reinhardt Wendorf & Blanchfield; Lockridge Grindal Nauen P.L.L.P.; Barrett Law Group, P.A.; Levin, Fishbein, Sedran & Berman; Kessler Topaz Meltzer & Check LLP; Carlson Lynch Ltd.; Scott + Scott LLP; Hausfeld LLP; and Beasley, Allen, Crow, Methvin, Portis Miles, P.C. as Co-Class Counsel. Chestnut Cambronne and Zimmerman Reed were previously appointed overall :*"4.&488(' lead counsel and lead of the Financial Institution Track 6+,N !#"@A19 of this MDL,

[118] Meet-and-Confer Statement, filed concurrently herewith.

respectively, and each of the other firms identified were appointed as Liaison Counsel and/or members of the FI Track executive or steering committee by the Court. ECF Nos. 64, 74, 436. Under Chestnut Cambronne and Zimmerman B%%I'(direction, each of these firms has diligently investigated and pursued the claims in this hard-fought litigation, which has survived !"#$%&'s motion to dismiss and involved complex discovery disputes (including motions to compel) and litigation around !"#$%&'(attempted settlement of Class claims with MasterCard. Collectively and individually, counsel has extensive experience managing and litigating complex class actions such as this one. Counsel is well familiar with the applicable law, as demonstrated by Plaintiffs' success in defeating Target's motion to dismiss. Finally, counsel's willingness to expend resources in the cause of this case is amply demonstrated. Rule 23(g) is satisfied.

IV. CONCLUSION

For the above-stated reasons, Plaintiffs respectfully request that the Court: (i) certify the Class; (ii) appoint Plaintiffs as representatives of the Class; and (iii) appoint Class Counsel as requested.

Dated: July 1, 2015

CHESTNUT CAMBRONNE PA

By: /s Karl L Cambronne
Karl L. Cambronne (MN 14321)
Jeffrey D. Bores (MN 227699)
Bryan L. Bleichner (MN 0326689)
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
kcambronne@chestnutcambronne.com
jbores@chestnutcambronne.com
bbleichner@chestnutcambronne.com

Coordinated Lead Counsel for Plaintiffs

ZIMMERMAN REED, PLLP

By: /s Charles S. Zimmerman
Charles S. Zimmerman (MN 120054)
J. Gordon Rudd, Jr. (MN 222082)
Brian C. Gudmundson (MN 336695)
1100 IDS Center, 80 South 8th St.
Minneapolis, MN 55402
Telephone: (612) 341-0400
charles.zimmerman@zimmreed.com
gordon.rudd@zimmreed.com
brian.gudmundson@zimmreed.com

Lead Counsel for Financial Institution Plaintiffs

REINHARDT WENDORF & BLANCHFIELD
Garrett Blanchfield
E-1250 First National Bank Building
332 Minnesota Street
St. Paul, MN 55101
Telephone: (651) 287-2100
g.blanchfield@rwblawfirm.com

Coordinating Liaison Counsel

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen Hanson Riebel
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com

Bank Liaison Counsel

LEVIN, FISHBEIN, SEDRAN & BERMAN
Howard J. Sedran
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
hsedran@lfsblaw.com

BARRETT LAW GROUP, P.A.
Don Barrett
404 Court Square North
PO Box 927
Lexington, MS 39092
Telephone: (662) 834-9168
dbarrett@barrettlawgroup.com

KESSLER TOPAZ MELTZER & CHECK LLP
Naumon A. Amjed
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
namjed@ktmc.com

CARLSON LYNCH LTD
Gary F. Lynch
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Telephone: (412) 322-9243
glynch@carlsonlynch.com

SCOTT + SCOTT LLP
Joseph P. Guglielmo
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Telephone: (212) 223-6444
jguglielmo@scott-scott.com

BEASLEY, ALLEN, CROW, METHVIN, PORTIS MILES, P.C.
W. Daniel Miles, III.
272 Commerce Street
PO Box 4160
Montgomery, AL 36103-4160
Telephone: (334) 269-2343
dee.miles@beasleyallen.com

HAUSFELD LLP
James J. Pizzirusso
1700 K Street NW, Suite 650
Washington D.C. 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeldllp.com

Plaintiffs Leadership Committee